

#4

Attorney Docket No. 225/49620  
PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

SPECIFICATION

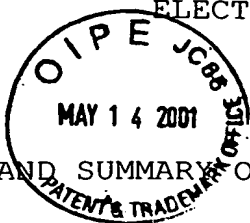
**INVENTION:** ELECTRONIC CONTROL SYSTEM

**INVENTOR:** Jochen RETTER  
Citizenship: German  
Residence/  
Post Office Address: Charlottenweg 4,  
73249 Wernau, GERMANY

**INVENTOR:** Anton RINK  
Citizenship: German  
Residence/  
Post Office Address: Rueppurrerstrasse 35  
76137 Karlsruhe, GERMANY

**ATTORNEYS:** EVENSON, McKEOWN, EDWARDS & LENAHAAN, P.L.L.C.  
Suite 700  
1200 G Street, N.W.  
Washington, D.C. 20005  
Telephone No.: (202) 628-8800  
Facsimile No.: (202) 628-8844

ELECTRONIC CONTROL SYSTEM



BACKGROUND AND SUMMARY OF THE INVENTION

[0001] This application claims the priority of German patent document 100 06 206.7, filed 11 February 2000, the disclosure of which is expressly incorporated by reference herein.

5 [0002] The invention relates to an electronic control system having a plurality of mutually networked or communicating control units, in which safeguards are provided to avoid incorrect response of a second control unit during the transmission of a safety-related signal from a first control unit to the second  
10 control unit.

[0003] Modern motor vehicles typically include complicated control systems which, in some circumstances, have many control units for actuating subsystems of the motor vehicle.

[0004] In distributed control systems used in known vehicle  
15 drive control systems, a first control unit calculates a desired variable in a higher-level control function. The desired variable is then transmitted via a data bus to a third control unit, which uses a lower-level control function to control a device based on the desired variable, such that the desired variable is optimally

set. The third control unit transmits an acknowledgment signal to the first control unit via a data bus.

[0005] For example, the control system can comprise an electronic engine controller and an electronic gearbox controller. In the event of a gear change, the gearbox controller transmits a signal to the engine controller as indicating a set point for the torque of the engine and, if appropriate, further set points for further parameters, for example the engine speed. This enables the engine controller to adopt operation of the engine to the gear change.

[0006] Control systems of this type must be secured against the generation and transmission of false signals in order to avoid the risk of serious malfunctions.

[0007] On the one hand, it is known in this context from International patent document WO 98/53374 to generate signals redundantly and, in the event of deviations between the redundantly determined results, to generate an error signal which has the effect of switching off the signal processing unit. On the other hand, WO 98/53374 also indicates a possibility of switching the control system to emergency operation upon detection of errors, so that the vehicle still remains ready for operation, although possibly at a reduced level of comfort.

[0008] One object of the present invention is to ensure particularly high operational reliability in a control system of the type mentioned previously.

[0009] This and other objects and advantages are achieved by the control system in which, according to the invention, during transmission of a safety-relevant transmitted signal from the first control unit to the second control unit,

- the first control unit generates the transmitted signal and a second signal complementary thereto on different paths (that is, in different modules), and sends them to a memory, together with two additional signals which are indicative of the paths;
- a third control unit reads out the transmitted signal and the second signal from the memory, and checks them, and, upon detection of an error, switches off the first control unit or, given correct signals, generates different types of test or safety signals and conducts them to a memory; and
- the first control unit reads out the test or safety signals from the last-named memory and checks them and, upon detection of an error, switches itself off, or, given correct test or safety signals, feeds the

transmitted signal and at least one prescribed selection of the test or safety signals to the second control unit.

5 [0010] The invention is based on the general idea that, before transmitting a safety-relevant signal to a second control unit, the first control unit cooperates with a third control unit for the purpose of checking the signal to be transmitted. The third control unit initially checks the function of the first control unit and, subsequently, the first control unit checks the  
10 function of the third control unit before the transmitted signal can be relayed to the second control unit. During this mutual checking, both the first and the third control units operate asymmetrically in a redundant fashion, the paths of the redundant signal generation also being checked.

15 [0011] Because the signals exchanged between the first and second control units are buffered in a memory, a delay which excludes undesired or parasitic instances of feedback between these control units occurs between the sending of a signal by one control unit and the reception of the signal at the other  
20 control unit.

[0012] In accordance with a particularly preferred embodiment of the invention, it is provided, furthermore, that the second control unit pays heed to the transmitted signal fed to it only

when it has recognized the test or safety signals further fed as error free.

[0013] In addition or as an alternative, the safety of the system can be further increased by providing that the second control unit returns the received transmitted signal as acknowledgment to the first control unit. In this manner, the function of the second control unit is also necessarily checked by another control unit, so that, upon detection of an error, undesired control functions cannot be triggered. Alternatively, it is possible to transfer to an emergency operating mode or standby operating mode of the control system.

[0014] Moreover, it can be provided that, when transmitting the signals to the second control unit, the first control unit reads back the signals to be transmitted, which were first input in a buffer, such that an additional signal comparison is provided here and the first control unit can be switched off again upon detection of an error.

[0015] Other objects, advantages and novel features of the present invention will become apparent from the following detailed description of the invention when considered in conjunction with the accompanying drawings.

## BRIEF DESCRIPTION OF THE DRAWINGS

[0016] The single figure shows a schematic block diagram of the electronic control system according to the invention, which control system preferably operates digitally.

## DETAILED DESCRIPTION OF THE DRAWINGS

[0017] The electronic control system 1 illustrated in the drawing has a data bus 2 via which different control units are mutually networked. In the example illustrated, the aim is for a first electronic control unit 3 (which may be, for example, an automatic gearbox controller in a motor vehicle) to send to a second electronic control unit 4 (for example, an electronic engine controller of the motor vehicle) safety-relevant signals representing, for example, the set point of an engine torque which is to be set in the event of a gear change in the gearbox.

[0018] According to the invention, the first control unit 3 initially generates an appropriate set point signal 5 and a set point signal  $S^*$  complementary thereof (for example bitwise), and feeds these signals to a memory 5. The set point signal  $S$  and the complementary set point signal  $S^*$  are generated by means of different modules of the hardware or software of the first control unit 3 -- that is, on different paths. Also, additional

signals Z, Z\* are generated, indicating the path used in each case, and are likewise fed to the memory 5.

5 [0019] A third electronic control unit 6, combined with the first control unit 3, thereupon reads the signals S, S\*, Z and Z\* from the memory 5, in order to carry out various test operations.

10 [0020] On the one hand, the complementary nature of the signals S and S\* can be checked, for example by adding these signals to one another in a bitwise fashion. If the bitwise addition then always leads to ZERO, the aforesaid bitwise complementary relationship is confirmed.

[0021] Furthermore, the value range of the signals S and S\* (that is, whether the signals lie in a permissible and/or plausible range) can be checked.

15 [0022] Moreover, the additional signals Z and Z\* can be checked for plausibility. For example, it can be provided that the paths used to generate the signals S and S\* in the first control unit 3 must be varied in accordance with prescribed time intervals. As a result, the third control unit 6 can, with the aid of the signals Z and Z\*, check the permissibility of the  
20 respective paths.

[0023] If the third control unit 6 establishes an error in the signals S, S\*, Z and/or Z\*, the first control unit 3 is switched off automatically. On the other hand, if the signals S, S\*, Z and Z\* are found to be error free, the third control unit 6 can calculate a parity signal (P or P\*, respectively), in relation to the digital signals S and S\*. The parity signal conveys how often the digital signals S and S\* contain a digital ONE. These parity signals are stored at different locations in the memory 5.

[0024] In addition, the third control unit 6 can generate so-called toggle bits T and T\* which can be complementary to one another in a prescribable way. These toggle bits are switched over at regular time intervals -- for example, in each case after a prescribed number of pulses of a central clock generator (not illustrated) of the control system 1. These clock generator pulses can be fed to the control units via separate signal lines (not illustrated).

[0025] The toggle bits T and T\* are also stored at different locations in the memory 5.

[0026] The first control unit 3 now reads out the parity signals P and P\* as well as the toggle bits T and T\* from the memory 5, and carries out various safety checks, for example an

addition test and plausibility tests. If an error is established, the first control unit 3 switches off.

[0027] If the first control unit 3 detects the aforementioned signals as being error free, it relays the set point signal S, the parity signal P and the toggle bit T to a buffer 7 which acts as a data bus transmitting unit and puts the aforementioned signals onto the data bus 2, to be received by the second control unit 4.

[0028] The second control unit 4 pays heed to the set point signal S only when the transmitted parity signal P correctly conveys the parity of the signal S, and also the toggle bit T is present and/or plausible. If these conditions are not fulfilled completely, the set point signal S is not accepted by the second control unit 4.

[0029] In parallel with the transmission of the signals S, P and T to the second control unit 4, these signals are also fed by the data bus 2 to a further buffer 8, which operates as a data bus receiving unit and returns the received signals to the first control unit 3. In this way, the first control unit 3 can check the agreement of the signals set by it with signals returned directly via the data bus 2. If a difference occurs, the first control unit 3 switches off.

[0030] Moreover, after receiving the signals S, P and T, the second control unit 4 can return to the first control unit 3 an acknowledgment signal having a structure dependent on the aforementioned signals. The received signal S, for example, can be sent as the acknowledgment signal. Should the first control unit 3 recognize the acknowledgment signal as defective (that is, as not corresponding to the signals S, P and T), this is the same as saying that a communication error is present.

[0031] In this case, the control system 1 can be switched over, as required, to emergency operation.

[0032] After the control unit 3 has been switched off automatically, if appropriate, or after it has been switched over to emergency operation, the control system 1 can be reset to normal operation again as part of service measures.

[0033] The elements 3 and 5 to 8 can be designed or programmed as parts or regions of a separate processor 9. In particular, the control units 3 and 6 can also be implemented in a single control unit as different software modules.

[0034] The data bus 2 can be provided as a so-called CAN bus, and the memory 5 is preferably a RAM.

[0035] In summary, the invention creates a logic system for monitoring desired variables in distributed control systems, in which it is possible to check the desired variables independently of the application.

5 [0036] The foregoing disclosure has been set forth merely to illustrate the invention and is not intended to be limiting. Since modifications of the disclosed embodiments incorporating the spirit and substance of the invention may occur to persons skilled in the art, the invention should be construed to include  
10 everything within the scope of the appended claims and equivalents thereof.